Ecole Nationale des Sciences Appliquées
Université Sidi Mohamed Ben Abdellah
Fès

2018-2019
Algèbre IV
CP2

EVALUATION DE FIN DE SEMESTRE
Session ordinaire (Durée : 2h00)

Exercice 1. On considère l'anneau $\mathbb{R}[X]$ des polynômes à coefficients dans $\mathbb{R}$. Soient $P = X^3 + X^2 + X + 1$ et $Q = X^3 - X^2 + X - 1$.

(1) Montrer $(P) + (Q) = (X^2 + 1)$ (Indication : vérifier que $\text{pgcd}(P, Q) = X^2 + 1$).

(2) On note $j = e^{2i\pi/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Nous rappelons que $j^2 + j + 1 = 0$.

(a) Montrer que l'application

$$\begin{array}{rccc} f: & \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ & P & \longmapsto & P(j) \end{array}$$

est un morphisme d'anneaux

(b) Montrer que f est surjectif (remarquer que $i = \frac{1}{\sqrt{3}} + \frac{2}{\sqrt{3}}j$).

(3) Montrer que $\ker(f) = (X^2 + X + 1)$ (considérer la division euclidienne de $P \in \ker(f)$ par le polynôme $X^2 + X + 1$).

(4) En déduire que $\mathbb{R}[X]/(X^2 + X + 1) \cong \mathbb{C}$.

(5) Que peut-on dire de l'idéal $(X^2 + X + 1)$ de $\mathbb{R}[X]$?

Exercice 2. On considère l'anneau $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ sur lequel on définit l'application norme N donnée par $N(a + ib) = |a + ib|^2 = a^2 + b^2 \in \mathbb{N}$.

(1) Vérifier que N est multiplicative.

(2) Déterminer les éléments inversibles de $\mathbb{Z}[i]$.

(3) Soient $x, y \in \mathbb{Z}[i]$ avec $y \neq 0$.

(a) Montrer qu'il existe $q \in \mathbb{Z}[i]$ tel que $\left|q - \frac{x}{y}\right| < 1$.

(b) On pose $r = x - qy$. Vérifier que $|r| < |y|$.

(c) Conclure que l'anneau $\mathbb{Z}[i]$ est Euclidien.

(d) Chercher une division euclidienne de $x = 5 + 6i$ par $y = 2 - 3i$ dans $\mathbb{Z}[i]$.

(4) Donner tous les diviseurs de $-1 + 3i$ dans $\mathbb{Z}[i]$.

(5) Donner tous les pgcd de $2i$ et $-1 + 3i$ dans $\mathbb{Z}[i]$.

Scanned with CamScanner

Examen algèbre

Ex 1 : On a : $P = X^3 + X^2 + X + 1$ et $Q = X^3 - X^2 + X - 1$

(1) Montrons que $(P) + (Q) = (X^2+1)$

On a :

$$\begin{array}{r|l} X^3+X^2+X+1 & X^2+1 \\ -X^3-X & \hline X+1 \\ \hline X^2-X & \\ -X^2-1 & \\ \hline -X-1+X+1 & \\ \hline 0 & \end{array}$$

et

$$\begin{array}{r|l} X^3-X^2+X-1 & X^2+1 \\ -X^3-X & \hline X-1 \\ \hline -X^2-X+X & \\ X^2+1 & \\ \hline 1-X & \\ \hline 0 & \end{array}$$

donc $P = (X^2+1)(X+1)$ et $Q = (X^2+1)(X-1)$

donc $(X^2+1) \mid P$ et $(X^2+1) \mid Q$ donc $\operatorname{pgcd}(P,Q) = X^2+1$

et soit M un polynome de $(P)+(Q)$ donc $\exists R, S \in \mathbb{R}[X]$ tq : $M = PR + QS$

d'où : $M = (X^2+1)(X+1)R + (X^2+1)(X-1)S \Rightarrow (X^2+1)\left((X+1)R + (X-1)S\right)$

on pose : $T = (X+1)R + (X-1)S$ et on a $T \in \mathbb{R}[X]$ donc $M = (X^2+1)T$

$\Rightarrow M \in (X^2+1)$ d'où A un polynome d'idéal engendré par le polynome X^2+1

• Inversement : soit A un polynome de (X^2+1) donc $\exists B \in \mathbb{R}[X]$

tq : $A = (X^2+1)B$ et comme $B \in \mathbb{R}[X]$ donc on peut écrire $B = R + S$ $R, S \in \mathbb{R}[X]$

avec $R = (X+1)R'$ et $S = (X-1)S'$

$$A = (X^2+1)\left((X+1)R' + (X-1)S'\right) = (X^3+X^2+X+1)R' + (X^3-X^2+X-1)S'$$
$$= PR' + QS'$$

d'où $A \in (P)+(Q) \Rightarrow (P)+(Q) = (X^2+1)$

(2) On a : $j = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ avec $j^2 + j + 1 = 0$

a- Montrons que : $f : \mathbb{R}[X] \longrightarrow \mathbb{C}$, $P \longmapsto P(j)$ est un morphisme d'anneaux

on a $f(0_{\mathbb{R}[X]}) = 0_{\mathbb{C}}$ et $f(1_{\mathbb{R}[X]}) = 1_{\mathbb{C}}$

et soient $P, Q \in \mathbb{R}[X]$ on a : $f(P+Q) = (P+Q)(j) = P(j) + Q(j) = f(P) + f(Q)$

$f(P \cdot Q) = (P \cdot Q)(j) = P(j) \cdot Q(j) = f(P) \cdot f(Q)$

$\longrightarrow$ d'où f est un morphisme d'anneaux car bien un morphisme.

Scanned with CamScanner

b) - Montrons que f est surjectif :

on a : $i = \frac{1}{\sqrt{3}} + \frac{2}{\sqrt{3}} j$ il suffit de montrer que : $\forall z = a+ib \in \mathbb{C}$

$\exists P \in \mathbb{R}[X]$ tq : $f(P) = z$

on a : $z = a+ib = a + \left(\frac{1}{\sqrt{3}} + \frac{2}{\sqrt{3}} j\right) b = a + \frac{b}{\sqrt{3}} + \frac{2b}{\sqrt{3}} j$

donc $\exists P(X) = a + \frac{b}{\sqrt{3}} + \frac{2b}{\sqrt{3}} X$ avec $f(P) = P(j) = z$

d'où f est surjectif.

3) - Montrons que : $\ker(f) = (X^2+X+1)$

soit $P \in \ker(f)$ donc : $f(P) = P(j) = 0$

on considère la division euclidienne de P sur X^2+X+1

donc $\exists Q, R$ tq : $P = (X^2+X+1)Q + R$ avec $\deg(R) < 2$ ou $R = 0$

on a : $P(j) = 0 = (j^2+j+1)Q + R = R \Rightarrow R = a \Rightarrow P = Q(X^2+X+1)$

donc $P \in (X^2+X+1)$ où (X^2+X+1) est l'idéal engendré par X^2+X+1.

Inversement soit $P \in (X^2+X+1)$. $\exists R \in \mathbb{R}[X]$ tq : $P = (X^2+X+1)R$

on a : $f(P) = P(j) = (j^2+j+1)R = 0$ donc $P \in \ker(f)$

$\Rightarrow \ker(f) = (X^2+X+1)$.

4) - on a : $f : \mathbb{R}[X] \to \mathbb{C}$ est un morphisme d'anneaux

donc d'après le 1er théorème d'isomorphisme on a : $\frac{\mathbb{R}[X]}{\ker(f)} \cong \mathrm{Im}(f)$.

or $\ker(f) = (X^2+X+1)$ et comme f est surjectif d'où : $\mathrm{Im}(f) = \mathbb{C}$

par suite $\frac{\mathbb{R}[X]}{(X^2+X+1)} \cong \mathbb{C}$.

6) - on a : $\frac{\mathbb{R}[X]}{(X^2+X+1)} \cong \mathbb{C}$ et $\mathbb{C}$ est un corps d'où $\frac{\mathbb{R}[X]}{(X^2+X+1)}$ l'est aussi

d'où (X^2+X+1) est un idéal maximal de $\mathbb{R}[X]$.

Ex 2

1) - on a : $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\}$ et $N(a+ib) = a^2+b^2 \in \mathbb{N}$

soient $z_1, z_2 \in \mathbb{Z}[i]$ avec $z_1 = a_1+b_1 i$ et $z_2 = a_2+b_2 i$

on a : $N(z_1 z_2) = N((a_1+b_1 i)(a_2+b_2 i)) = N(a_1a_2 - b_1b_2 + i(a_1b_2 + b_1a_2))$

$= (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2 = (a_1a_2)^2 + (b_1b_2)^2 - 2a_1a_2b_1b_2$

$+ (a_1b_2)^2 + 2a_1a_2b_1b_2 + (b_1a_2)^2 = (a_1a_2)^2 + (b_1b_2)^2 + (a_1b_2)^2 + (b_1a_2)^2$

$= a_2^2(a_1^2 + b_1^2) + b_2^2(b_1^2 + a_1^2) = (a_1^2+b_1^2)(a_2^2+b_2^2)$

$= N(z_1) \cdot N(z_2)$ d'où N est multiplicative.

Scanned with CamScanner

2) - soit $z \in \mathbb{Z}[i]$ on a : z est inversible si $\exists z' \in \mathbb{Z}[i]$ tq : $zz' = 1$

d'où $N(zz') = 1 \Rightarrow N(z) \cdot N(z') = 1$ or $N(z), N(z') \in \mathbb{N}$

donc $N(z) \in 1$ et comme $z \in \mathbb{Z}[i]$: $\exists a, b \in \mathbb{Z}$: tq : $z = a + ib$

donc $N(z) = a^2 + b^2 = 1$: les cas possibles sont : $(a = \pm 1$ et $b = 0)$

ou $(a = 0$ et $b = \pm 1)$ donc on a $z = \pm 1$ et $z = \pm i$

Inversement $N(\pm 1) = 1$ et $N(\pm i) = 1$

donc les éléments inversibles de $\mathbb{Z}[i]$ sont : $\{\pm i, \pm 1\} \Rightarrow U(\mathbb{Z}[i]) = \{\pm i, \pm 1\}$

3) - soient $x, y \in \mathbb{Z}[i]$ avec $y \neq 0$:

(a) - on a : $\frac{x}{y} = \alpha + i\beta$ avec $\alpha, \beta \in \mathbb{R}$ (l'écriture algébrique de $\frac{x}{y}$)

on pose $q = u + iv$ avec u le plus proche à α et v l'entier le plus proche au réel β donc : on a : $|u - \alpha| < \frac{1}{2}$ et $|v - \beta|$

donc $|q - \frac{x}{y}|^2 = |u + iv - (\alpha + i\beta)|^2 = (u - \alpha)^2 + (v - \beta)^2 < \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$

donc $|q - \frac{x}{y}|^2 < 1 \Rightarrow |q - \frac{x}{y}| < 1$

(b) - on pose $r = x - qy$ on a : $|y| \, |q - \frac{x}{y}| < |y|$

$\Rightarrow |qy - x| < |y| \Rightarrow |x - qy| < |y| \Rightarrow |r| < |y|$

(c) - • soit $z_1, z_2 \in \mathbb{Z}[i]$. on a : $z_1 | z_2 \Rightarrow \exists z_3 \in \mathbb{Z}[i]$ tq

$z_2 = z_1 z_3 \Rightarrow N(z_2) = N(z_1) N(z_3)$ et comme la norme est positive toujours : donc $N(z_1) < N(z_2)$.

• d'après a) et b) on a : pour tout $x, y \in \mathbb{Z}[i]$: $\exists q, r$: $x = qy + r$ avec $|r| < |y|$

• ou $\mathbb{Z}[i]$ est une anneau euclidien pour la norme $|\cdot|$

(d) - on a : $x = 5 + 6i$ et $y = 2 - 3i$ on procède de la même manière que $q = a$ et $q = b$:

on a : $y \neq 0$: donc $\frac{x}{y} = \frac{5 + 6i}{2 - 3i} = \frac{(5 + 6i)(2 + 3i)}{4 + 9} = \frac{10 - 18 + i\,27}{13} = \frac{-8}{13} + \frac{27}{13} i$

on remarque que $\frac{-8}{13}$ est le plus proche à -1 et $\frac{27}{13}$ est le plus proche à 2 avec $|\frac{-8}{13} - (-1)| < \frac{1}{2}$ et $|\frac{27}{13} - 2| < \frac{1}{2}$

donc on a $q = -1 + 2i$ et $r = x - qy = 5 + 6i - (2 - 3i)(-1 + 2i)$

$r = 5 + 6i - (-2 + 4i + 3i + 6) = 5 + 6i - (4 + 7i) = 5 + 6i - 4 - 7i = +1 - i$

donc pour $x = 5 + 6i$ et $y = 2 - 3i$ $\exists q, r \in \mathbb{Z}[i]$ tq : $q = -1 + 2i$

et $r = 1 - i$ avec : $x = qy + r$

Verification : $qy + r = (-1 + 2i)(2 - 3i) + (1 - i) = -2 + 6 + 7i + 1 - i = 5 + 6i = x$ ∎

(4) les diviseurs de $-1+3i$ dans $\mathbb{Z}[i]$ soit $z \in \mathbb{Z}[i]$ tq $z = a+ib$.

on a : $z \mid -1+3i$ si et seulement $\exists z' \in \mathbb{Z}[i]$ tq $-1+3i = zz'$

$\Rightarrow N(zz') = 10 \Rightarrow N(z)N(z') = 10 \Rightarrow N(z) \in \{1, 10, 2, 5\}$

• $N(z) = 1 \Rightarrow a^2+b^2 = 1 \Rightarrow a \in \{0,1,-1\}$ et $b \in \{0,1,-1\}$ c.a.d les cas possibles sont : $(1,0)$ $(-1,0)$, $(0,1)$, $(0,-1)$ donc $z_1 = 1$ et $z_2 = -1$, $z_3 = i$; $z_4 = -i$

• $N(z) = 10 \Rightarrow a^2+b^2 = 10 \Rightarrow$ les cas possibles sont : $(-1,3)$ $(-1,-3)$ $(3,1)$ $(-3,1)$ et $(-1,3)$ $(+1,-3)$, $(3,-1)$ $(-3,1)$ donc $z_5 = 1+3i$, $z_6 = -1-3i$; $z_7 = 3+i$, $z_8 = -3$

$z_9 = -1+3i$, $z_{10} = 1-3i$, $z_{11} = 3-i$; $z_{12} = -3+i$

• $N(z) = 2 \Rightarrow a^2+b^2 = 2 \Rightarrow$ les cas possibles sont $(1,1)$ $(-1,-1)$ $(1,-1)$ $(-1,$

donc $z_{13} = 1+i$ et $z_{14} = -1-i$, $z_{15} = 1-i$, $z_{16} = -1+i$

• $N(z) = 5 \Rightarrow a^2+b^2 = 5 \Rightarrow$ les cas possibles : $(2,1)$ $(-2,-1)$ $(1,2)$ $(-1,-2$

$(-1,2)$ $(1,-2)$ $(2,-1)$ $(-2,1)$ donc $z_{17} = 2+i$, $z_{18} = -2-i$, $z_{19} = 1+2i$

$z_{20} = -1-2i$, $z_{21} = -1+2i$, $z_{22} = 1-2i$, $z_{23} = 2-i$, $z_{24} = -2+i$

on pose $z = -1+3i$

Scanned with CamScanner

• Inversement on a: $z_1 z_9 = z$, $z_2 z_{10} = z$, $z_3 z_{11} = z$, $z_4 z_{12} = z$.
$z_{13} z_{19} = z$, $z_{14} z_{20} = z$, $z_{15} z_{24} = z$ et $z_{16} z_{23} = z$
et pour $z_5, z_6, z_7, z_8, z_{17}, z_{18}, z_{21}, z_{22}$ le sens inverse
n'est pas correct, ex: $z_{22} = 1-2i$ on a: $(1-2i)(a+ib) = -1+3i$
$\Rightarrow \begin{cases} a+2b=-1 \\ 2a+b=3 \end{cases} \Rightarrow b = 7+2a \Rightarrow 5a = -7$ absurde.
Donc les diviseurs de $-1+2i$ sont $\{\pm i, \pm 1, \pm(-1+2i), \pm(2-i), \pm(1+i), \pm(1-i)$
$\pm(1+2i), \pm(2-i)\}$

(3) les diviseurs de $2i$.
soit $z = a+ib \in \mathbb{Z}[i]$ on a: $z / 2i$ si $\exists z' \in \mathbb{Z}[i]$ tq: $zz' = 2i$
$\Rightarrow N(zz') = 4 \Rightarrow N(z) \in \{1; 2; 4\}$
• $N(z) = 1 \Rightarrow$ les cas possible: $(0,1), (1,0), (-1,0), (0,-1)$
donc $z_1 = 1$, $z_2 = -1$, $z_3 = i$, $z_4 = -i$
• $N(z) = 2 \Rightarrow a^2+b^2 = 2$ les cas possible $(1,1), (-1,-1), (1,-1), (-1,1)$
donc $z_5 = 1+i$, $z_6 = -1-i$, $z_7 = 1-i$, $z_8 = -1+i$
• $N(z) = 4 \Rightarrow a^2+b^2 = 4$: les cas possible: $(0,2), (2,0), (-2,0), (0,-2)$
donc $z_9 = 2i$, $z_{10} = 2$, $z_{11} = -2$, $z_{12} = -2i$
Inversement on a: $z = 2i$: $z_1 z_9 = z$; $z_2 z_{12} = z$; $z_3 z_{10} = z$, $z_4 z_{11} = z$
$z_5 z_7 = (1+i)^2 = 1+2i-1 = z$; $z_6^2 = z$, $z_7 \times z_8 = (1-i)(-1+i) = z$
donc les diviseurs de $2i$ sont $\{\pm 1, \pm i, \pm(1+i); \pm(1-i), \pm 2, \pm 2i\}$

les diviseurs communs de $-1+3i$ et $2i$ sont: $\{\pm 1, \pm i, \pm(1+i), \pm(1-i)\}$
or on a: $1(1+i) = (1+i)$ et $-1(-1-i) = (1+i)$ et $i(1-i) = i+1$
et $-i(i-1) = (1+i)$ (même pour $(-1-i)$)
et $1(i-1) = (i-1)$, $-1(1-i) = (i-1)$ et $+i(1+i) = (i-1)$ et $-i(-1+i) = (i-1)$
même pour $(1-i)$

Donc $\text{pgcd}(-1+3i, 2i) = \{\pm(1+i), \pm(1-i)\}$